UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/038,752	12/31/2001	C. Andrew Neff	324628006US1	6285

25096 7590 06/20/2005

PERKINS COIE LLP
PATENT-SEA
P.O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/038,752	NEFF, C. ANDREW	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-12* is/are allowed.

6)☒ Claim(s) *13-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 12/6/04, 8/16/04, 5/20/04, 1/20/04, 6/27/03 11/12/02, 10/24/02, 9/26/02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: (150) and (311). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: (130). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application.

Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 38 and 39 contain the limitations wherein the confirmation sent from the second computer system is encrypted in such a way that its decryption by the second computer system is infeasible/impossible. There is a lack of antecedent basis for these limitations as claimed.

Allowable Subject Matter

Claims 1 – 12 are allowed.

The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 1, what is claimed is a data processing system for discerning corruption of an electronic ballot.

In a first aspect, the system as claimed comprises the sending of an encrypted ballot and a validity proof (a proof showing that the ballot is valid), from a voter computer system to a vote collection center computer system. The vote collection center computer system receives the encrypted ballot and validity proof, verifies the validity proof, and if the ballot is valid, generates an encrypted vote confirmation without

decrypting the encrypted ballot, and sends the vote confirmation to the voter computer system. The voter computer system receives the encrypted vote confirmation, decrypts the confirmation, and displays the confirmation to the user.

In a second aspect, the system as claimed further comprises a confirmation dictionary in the user's possession, which is used to translate the vote confirmation received from the vote collection computer system to the ballot choice selected by the voter. If the vote confirmation received by the voter computer system does not equal an entry in the confirmation dictionary indicating the voter's ballot choice, then the voter can determine that the ballot had been corrupted.

Examiner points out that the "confirmation dictionary" does not have an accepted meaning in the art. As shown by the applicant, the claimed confirmation dictionary includes at least a data structure (i.e. table) containing a plurality of values each corresponding to a possible ballot choice, and containing one value equaling the received vote confirmation only if the ballot had not been corrupted. The claimed confirmation dictionary is unique per voter, generated by the vote collection computer system using random and independent values, secret to and uniquely generated by the vote collection computer system for each voter. Further, the claimed confirmation dictionary is distributed by the vote collection computer system to each voter (Instant Application, page 6, lines 1-4; page 7, lines 1-8; page 10, line 29 – page 11, line 2; page 14, lines 1-3; page 18, lines 17-19).

Prior Art teaches or suggests elements of the first aspect of the claimed invention. Namely the sending of encrypted ballots and ballot validity proofs and the

generating of a type of vote confirmation that may be used by the voter to confirm that a vote has been correctly received and/or counted by an electronic voting system (Kilian et al. - "Secure Electronic Voting Using Partially Compatible Homomorphisms" (U.S. Patent, 5,495,532), Fujioka et al. - "Electronic Voting Method and System and Recording Medium Having Recorded Thereon a Program for Implementing the Method" (U.S. Patent 6,845,447 B1), Cranor - "Electronic Voting", Cramer et al. - "A Secure and Optimally Efficient Multi-Authority Election Scheme", Cramer et al. - "Multi-Authority Secret-Ballot Elections with Linear Work", and Borrell et al. - "An Implementable Secure Voting Scheme"). However, the Prior Art does not teach or suggest the combination of the first and second aspects of the invention as claimed, including the confirmation dictionary.

Regarding claims 2 – 11, they are dependent upon and further limit claim 1.

Regarding claim 12, it is substantially similar to claim 1, being content on a computer readable medium that performs the functions indicated by the method claim 1, and is allowable for the same reasons.

Claims 31 and 36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 24 – 28, and 34 – 36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claim 24, it is addressed to memories storing "secrets". The "secrets" are non-functional descriptive material, directed to data, *per se*. The secrets do not constitute data structures, since there are no claimed functional interrelationship between data elements.

Regarding claim 25 – 28, they are addressed to memories containing a ballot, proof of validity, and a ballot confirmation. Such are non-functional descriptive material, directed to data, per se. Such stored data does not constitute a data structure.

Claims 34 –36 are directed towards data signals and thus are rejected as not being tangible.

To expedite a complete examination of the instant application, it is presumed that the claims rejected under 35 USC § 101 above will be amended so as to place them within a statutory category.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 13 – 30, 32 – 35, and 37 – 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme".

Regarding claim 13, Cramer et al. discloses:

using a secret maintained in the voting node to encrypt a ballot value selected by a voter; sending the encrypted ballot value to a vote collection point (Cramer et al., page 1, par. 3 – page 2, par. 3);

Cramer et al. discloses the generating from the encrypted ballot (and other encrypted ballots) an election tally – "vote confirmation" - (Cramer et al., page 2, lines 1-21; page 7, par. 1), which would be published to the participants and observers of the electronic voting system (Cramer et al., page 9, pars. 3, 4). Voters can then reference

the published encrypted ballots of the system bulletin board so as to compute the tally and compare the computed result to the published confirmation result. The correspondence between the computed tally from the bulletin board and the published tally from the vote collection system expresses the confirmation to the voter that his/her vote has or has not been corrupted. For example, a voter may access his posted ballot, use it to compute the election tally, and compare the results. If the computed tally equaled the posted tally, then voter can be assured that his vote, at least, was not corrupted (Cramer et al., page 2, lines 1-21). Cramer et al. does not disclose that the vote confirmation has been encrypted by the vote collection system and decrypted by the voter computer system using a secret.

Cramer et al., however, disclose that the electronic voting system bulletin board is used by participants to send messages. Participants – not observers – can post messages to their assigned area of the bulletin board. In order to verify posted messages, the public key infrastructure and, specifically, digital signatures (encryption with the private key) is used (Cramer et al., page 2, par. 2; page 4, pars. 3,4).

It would have been obvious to one of ordinary skill in the art to employ the encryption and decryption of the vote confirmation with the electronic voting system of Cramer et al. The vote collection system would digitally sign (encrypt with a private key) and post the vote confirmation, and the voter computer system would access and verify (decrypt with the publicly available public key) the vote confirmation. This would have been obvious because one of ordinary skill in the art would have been motivated to enable public verifiability of posted messages using the public key infrastructure (i.e.

digital signatures) as taught by Cramer et al., and thereby allow voters to confirm that the vote confirmation was in fact computed by the vote collection computer.

Regarding claim 14, the modification of Cramer et al., discloses:

further comprising before displaying the decrypted vote confirmation, using a hash function to transform the decrypted vote confirmation into a smaller hash output value (Cramer et al., page 6-7, sect. 2.4).

Regarding claim 15, the modification of Cramer et al., discloses:

wherein encrypting the ballot value comprises generating an ElGamal pair representing the ballot value (Cramer et al., page 5).

Regarding claim 16, the modification of Cramer et al., discloses:

wherein the ElGamal pair is generated by evaluating the expressions g^{α} *and* h^{α} + *m , where p is prime', g I* Z_p *, which has prime multiplicative order q, with the property that q is a multiplicity 1 divisor of p – 1; h ϵ {L} ; a ϵ Zq is chosen randomly at the voting node; and m is the ballot value* (Cramer et al., page 4, 5, sects. 2.2, 2.3).

Regarding claim 17, the modification of Cramer et al., discloses:

wherein the ElGamal pair is generated by evaluating the expressions αg and αh+m , where g and h are both elements of an elliptic curve group, ϵ , of prime order q

and α ϵ Zq is chosen randomly at the voting node, and m is the ballot value (Cramer et al., page 4, 5, sects. 2.2, 2.3).

Regarding claim 18, the modification of Cramer et al., discloses:

determining the ballot value corresponding to the encrypted ballot value received at the vote collection point by evaluating the expression $W_l/U_l^{\alpha l}$ *,where* α_l *is the secret maintained in the voting node, and* W_l *and* U_l *together comprise the encrypted vote confirmation; and comparing the determined ballot value to the ballot value selected by the voter* (Cramer et al., page 5-6, sect 2.3; page 7-8, sect. 2.6).

Regarding claim 19, the modification of Cramer et al., discloses:

sending to the vote collection point a validity proof proving that the encrypted ballot value corresponds to a valid ballot value (Cramer et al., page 1, par. 3 – page 2, par. 3).

Regarding claim 20, the modification of Cramer et al., discloses:

wherein the validity proof is a non-interactive proof of validity (Cramer et al., page 6-7, sect. 2.4).

Regarding claim 21, it is rejected as being the method of claim 13 embodied in a computer readable medium. The modification of Cramer et al. discloses an electronic voting system comprising computers ("nodes") to execute the method of claim 13. It is

inherent that these computers contain computer readable medium embodying the method of claim 13 so as to accomplish what is disclosed.

Regarding claim 22, it is rejected for the same reasons as claim 13.

Regarding claim 23, the modification of Cramer et al. discloses:

the contents of the computer-readable medium further cause the voting node to send to the vote collection point a validity proof proving that the encrypted ballot value corresponds to a valid ballot value (Cramer et al., page 1, par. 3 – page 2, par. 3).

Regarding claim 24, the modification of Cramer et al., discloses:

One or more computer memories collectively containing a voter security data structure, the data structure containing one or more secrets usable both (a) to encrypt an encoded ballot for transmission to a ballot collection point, and (b) to decrypt an encrypted ballot confirmation received from the ballot collection point, which indicates the contents of the ballot as received at the ballot collection point (Cramer et al., page 1; par. 2 – page 2; page 4 – 5, section 2.2; page 3, par. 4; page 4, par. 3;). The modification of Cramer et al. discloses the processes of encrypting a ballot and decrypting a vote confirmation using secrets. It is inherent that these secrets be contained in memory so as to be used when needed for these processes.

Regarding claim 25, the modification of Cramer et al., discloses:

One or more computer memories collectively containing a ballot data structure, the ballot data structure comprising: an encrypted ballot choice formed by encrypting one of a plurality of valid ballot choices selected by a voter in a voter computer system; a proof of validity that demonstrates that the encrypted ballot choice constitutes an encryption of one of the plurality of valid ballot choices without indicating which of the plurality of valid ballot choices the encrypted ballot choice constitutes an encryption of; and an encrypted ballot confirmation generated in response to the receipt in a ballot collection center computer system of the encrypted ballot choice and proof of validity (Cramer et al., page 4, sect. 2.1). The modification of Cramer et al. discloses the use of a bulletin board (accessible by all participants to the voting system) where all messages of the participants will be posted, including the encrypted ballots, validity proofs, and vote confirmation.

Regarding claim 26, it is rejected for the same reasons as claim 15.

Regarding claims 27 and 28, they are rejected for the same reasons as claim 25.

Regarding claim 29, the modification of Cramer et al., discloses:

receiving an encrypted ballot value from a ballot sending node, the encrypted ballot value being encrypted from a ballot value based on a voter selection using a secret not available in the ballot receiving node (Cramer et al., page 3, par. 4; page 5, par. 5; page 9, par. 4);

generating from the encrypted ballot value an encrypted secret value confirmation that indicates to those in possession of the secret used to encrypt the encrypted ballot value the ballot value to which the received encrypted ballot value corresponds; and sending the encrypted secret value confirmation to the ballot sending node, such that the encrypted secret value confirmation may be used in the ballot sending node to determine if the encrypted ballot value received at the ballot receiving node corresponds to the ballot selection made by the voter (Cramer et al., page 2, lines 1-21; page 7, par. 1; page 9, pars. 3, 4).

Regarding claim 30, the modification of Cramer et al. discloses:

wherein the secret value confirmation is generated without decrypting the encrypted ballot value (Cramer et al, page 2, lines 1-21; page 14, par. 2, lines 1-9).

Regarding claim 32, the modification of Cramer et al., discloses:

wherein the encrypted secret value confirmation is encrypted in such a manner that, in the ballot sending node, given the encrypted secret value confirmation corresponding to a selection other than the voter selection, it is intractable to generate a decrypted secret value confirmation corresponding to the voter selection (Cramer et al., page 4, sect. 2.2). As disclosed, the election scheme of Cramer et al. prevents cheating.

Regarding claim 33, it is the apparatus claim corresponding to the method claim of 29, and is rejected for the same reasons. Further, the modification of Cramer et al., discloses an "authority" system for executing the method of claim 29. An authority that receives a ballot, generates a confirmation, and sends the confirmation, must contain a means to receive, generate, and transmit (Cramer et al., page 9, pars. 3,4).

Regarding claim 34, the modification of Cramer et al., discloses:

one or more generated data signals collectively conveying a ballot response data structure containing an encrypted ballot confirmation generated in response to the receipt at a ballot collection point of a ballot cast by a voter, the encrypted ballot confirmation, when decrypted on behalf of the voter, indicating a voting selection made by the voter in the cast ballot as received at the ballot collection point (Cramer et al, page 9, par. 3; page 2, par. 1; page 4, sect. 2.1). As disclosed by the modification of Cramer et al., the data structures containing the generated ballot confirmation are posted to the bulletin board. Thus, disclosed are the posts "generated data signals" that contain the ballot response data structure.

Regarding claim 35, the modification of Cramer et al., discloses:

wherein the ballot received at the ballot collection point is encrypted, and wherein the encrypted ballot confirmation is generated without decrypting the encrypted ballot (Cramer et al., page 1, par. 3 – page 2, par. 3; page 9, par. 4; page 14, par. 2, lines 1-9).

Regarding claim 37, the modification of Cramer et al., discloses:

sending an encrypted ballot from a first computer system to a second computer system, the encrypted ballot reflecting a ballot choice selected by a voter (Cramer et al., page 1, par. 3 – page 2, par. 3);

sending a confirmation from the second computer system to the first computer system, the confirmation serving to convey the decrypted contents of the encrypted ballot as received at the second computer system, the confirmation being generated without decrypting the encrypted ballot; and in the first computer system, displaying the confirmation, so that the voter can determine whether the decrypted contents of the encrypted ballot as received at the second computer system match the ballot choice selected by the voter (Cramer et al., page 9, par. 4; page 14, par. 2, lines 1-9; see also rejection of claim 13).

Regarding claim 38, the modification of Cramer et al., discloses:

wherein the confirmation sent from the second computer system to the first computer system is encrypted in such a manner that its decryption by the second computer system is infeasible (Cramer et al., page 2, lines 1-25).

Regarding claim 39, the modification of Cramer et al., discloses:

wherein the confirmation sent from the second computer system to the first computer system is encrypted in such a manner that its decryption by the second computer system is impossible (Cramer et al., page 2, lines 1-25).

Regarding claim 40, the modification of Cramer et al., discloses:

sending from the first computer system to the second computer system a validity proof proving that the encrypted ballot sent from the first computer system to the second computer system reflects a valid ballot choice without identifying the reflected ballot choice (Cramer et al., page 2, lines 1-30).

Regarding claim 41, the modification of Cramer et al. discloses:

wherein the confirmation is sent from the second computer system to the first computer system only if the validity proof sent from the first computer system to the second computer reflects a valid ballot choice (Cramer et al, page 14, par. 2, lines 1-9; page 9, pars. 3,4). The modification of Cramer et al. discloses that only valid ballots are tallied and thus would be included in the confirmation post to the bulletin board.

Regarding claim 42, it is rejected as being the method of claim 37 embodied in a computer readable medium. The modification of Cramer et al. discloses an electronic voting system comprising computers to execute the method of claim 37. It is inherent that these computers contain computer readable medium embodying the method of claim 37 so as to accomplish what is disclosed.

Regarding claim 43, it contains substantially the same limitations as claim 40 and is rejected for the same reasons.

Regarding claim 44, it contains substantially the same limitations as claim 41 and is rejected for the same reasons.

Regarding claim 45, it contains substantially the same limitations as claim 13 and is rejected for the same reasons.

Regarding claim 46, it contains substantially the same limitations as claims 13 and 21 and is rejected for the same reasons.

Regarding claim 47, the modification of Cramer et al., discloses:

receiving the electronic ballot, the electronic ballot containing an encrypted ballot choice; determining that the received encrypted ballot choice is not accompanied by a valid validity proof that proves that the encrypted ballot choice constitutes the encryption of one of a plurality of permissible ballot choices; and in response to so determining, determining that the generated first ballot has been compromised (Cramer et al, page 2, par. 2; page 9, par. 4; page 14, par. 2, lines 1-9).

Regarding claim 48, the modification of Cramer et al., discloses:

wherein no validity proof is received for the encrypted ballot choice (Cramer et al., page 12, par. 8).

Regarding claim 49, the modification of Cramer et al., discloses:

wherein a validity proof is received along with the encrypted ballot choice, and the combination of validity proof and encrypted ballot fail a verification operation performed by the vote collection computer system, where the verification operation is constructed explicitly to determine whether the encrypted ballot is an encryption of at least one of the valid ballot responses (Cramer et al., page 12-13, sect. 6.1).

Regarding claim 50, the modification of Cramer et al., discloses:

means for receiving the electronic ballot, the electronic ballot containing an encrypted ballot choice (Cramer et al., page 2, lines 1-25)*; means for determining that the received encrypted ballot choice is not accompanied by a valid validity proof that proves that the encrypted ballot choice constitutes the encryption of one of a plurality of permissible ballot choices; and means for, in response to so determining, determining that the generated first ballot has been compromised* (Cramer et al., page 2, lines 1-25; page 7, par. 4; page 8, fig. 2). The modification of Cramer et al. discloses a means for the verifier or ballot collection system to check and verify the validity of votes so as to prevent disruption from voters who submit invalid votes (Cramer et al., page 14, par. 2).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Bruce Schneier, Applied Cryptography, Second Edition, 1996, John Wiley & Sons Inc., pages 476 – 481, 490-1, 532-3.

Hall et al., "Voting Method and System", U.S. Pub. 2002/0074399 A1.

Karro et al., "Electronic Voting System", U.S. Pub. 2002/0077885 A1.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Jeffery Williams
Assistant Examiner
Art Unit 2137